IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Alexandria Division

ADBULKADIR NUR,	)	
	)	
Plaintiff,	)	
	)	
v.	)	Civil Action No. 1:22-cv-169 (AJT/JFA)
	)	
UNKNOWN CBP OFFICERS, *et al.*,	)	
	)	
Defendants.	)	
	)	
	)	
	)	
	)	

MEMORANDUM IN SUPPORT OF OFFICIAL CAPACITY DEFENDANTS' MOTION TO DISMISS

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES

STATUTES

RULES

REGULATIONS

UNITED STATES CONSTITUTION

OTHER AUTHORITIES

INTRODUCTION

Plaintiff Abdulkadir Nur alleges that he is on a federal terrorist watchlist and, as a result, U.S. Customs and Border Protection ("CBP") officers have subjected him to secondary screening and electronic device searches when he arrives in the United States. He brings claims under the Fourth Amendment, the Fifth Amendment's Self-Incrimination Clause, and the Administrative Procedure Act ("APA").[1] Pursuant to Federal Rule of Civil Procedure 12(b)(6), Defendants Chris Magnus, CBP Commissioner, and Christopher Wray, the Director of the Federal Bureau of Investigation ("FBI"), in their official capacities, move to dismiss Counts I, II, and III.

Although the nature of his claims is unclear, Plaintiff appears to bring both facial and as-applied claims under the Fourth Amendment arising from these border inspections. *See* Compl. ¶¶ 97-119 (asserting claims on behalf of himself and "similarly situated Americans"), ECF No. 1; *id.* ¶¶ 75-95 (detailing factual allegations pertaining only to Plaintiff). Plaintiff's facial claims suffer from a variety of defects and are subject to dismissal *ab initio*. To begin, CBP border inspections are governed by settled, written policies, with which Plaintiff appears not to take material issue. Instead, Plaintiff launches a vague, programmatic challenge to "CBP policies" that he claims exist based on extrapolations from his various encounters at the border. Plaintiff's speculations are simply insufficient to infer the existence of such imagined policies. The actual policies that CBP follows are entirely proper, and Plaintiff's facial challenge falls woefully short of establishing that

[1] Plaintiff also brings a count under *Bivens v. Six Unknown Named Agents of Federal Bureau of Narcotics*, 403 U.S. 388 (1971), against unknown CBP Officer Defendants. Compl. ¶¶ 133-37. Counsel does not represent the Unknown CBP Officer Defendants. This motion is only being filed on behalf of the listed official-capacity Defendants. The official-capacity Defendants note, however, that under recent Supreme Court precedent, Plaintiff's individual-capacity claims pursuant to *Bivens* would be foreclosed. *See Egbert v. Boule*, 142 S. Ct. 1793, 1806 (2022) ("[W]e ask here whether a court is competent to authorize a damages action . . . against Border Patrol agents generally. The answer, plainly, is no.").

"no set of circumstances exists under which the [policies] would be valid." *United States v. Salerno*, 481 U.S. 739, 745 (1987).

His as-applied Fourth Amendment claim for prospective relief[2] likewise falls short. Subject to a few narrow exceptions, the Fourth Amendment permits customs officers to conduct border searches, such as secondary inspections and manual searches of electronic devices, without any heightened suspicion. And Plaintiff has not plausibly alleged that CBP officers lacked reasonable suspicion to conduct forensic searches of his electronic devices—much less that CBP officers would lack such suspicion in the future, such that he would be entitled to injunctive relief.

Plaintiff's Fifth Amendment claim also fails as a matter of law. Plaintiff contends that CBP officers' request that he provide his passwords and biometric information to unlock his cell phone violates his right against self-incrimination, but "it is not until [a statement's] use in a criminal case that a violation of the Self-Incrimination Clause occurs." *Chavez v. Martinez*, 538 U.S. 760, 767 (2003). This is a civil case—brought by Plaintiff—and Plaintiff has not claimed that he is subject to any impending criminal proceeding. Further, he does not allege that any information contained on his devices could be incriminating. Finally, even if actionable, the remedy for a violation of the Self-Incrimination Clause is the exclusion of evidence from a criminal proceeding, not injunctive or declaratory relief of the type sought here. *See Michigan v. Tucker*, 417 U.S. 433, 451-52 (1974).

Plaintiff's APA claim likewise fails. His APA claim is coextensive with, and therefore should suffer the same fate as, his insufficient constitutional claims. Moreover, the APA only permits challenges to discrete, final agency action, not the sort of broad, programmatic challenge Plaintiff attempts to mount based on extrapolations and inferences that do not reflect CBP's actual,

[2] The claims against the agency defendants are for prospective relief only.

stated policies. Even if his APA claim were cognizable, Plaintiff merely recites the elements of an APA cause of action in a conclusory fashion, which is inadequate under Rule 12(b)(6).

Finally, buried in his prayer for relief, Plaintiff appears to directly challenge the basis for the alleged watchlist status upon which he grounds all his claims. But this demand is untethered from any viable claim for relief and therefore provides no basis to allow this action to proceed, even on that narrow ground.

For the reasons set forth below, the Court should dismiss Counts I, II, and III against the official capacity defendants.

BACKGROUND

I. The Government's Watchlisting Policies and CBP's Authority

Several different components within the federal government secure the United States and its aviation system from terrorist threats. The FBI investigates and analyzes intelligence relating to both domestic and international terrorist activities, *see* 28 U.S.C. § 533, 28 C.F.R. § 0.85(l), and administers the Terrorist Screening Center ("TSC"). *See* Homeland Security Presidential Directive/HSPD-6 ("HSPD-6") (Sept. 16, 2003), https://www.gpo.gov/fdsys/pkg/PPP-2003-book2/pdf/PPP-2003-book2-doc-pg1174.pdf (last visited July 10, 2022).

The Department of Homeland Security ("DHS") is charged with "prevent[ing] terrorist attacks within the United States," 6 U.S.C. § 111(b)(1)(A), and "reduc[ing] the vulnerability of the United States to terrorism," *id.* § 111(b)(1)(B); *see also* 6 U.S.C. § 202(1). Within DHS, CBP has broad authority under numerous statutes to inspect all persons and goods entering the United States. *See, e.g.,* 6 U.S.C. § 211; 8 U.S.C. § 1357; 19 U.S.C. §§ 482, 1455, 1459, 1461, 1467, 1499, 1581, 1582. These authorities include, but are not limited to, inspections for the purpose of preventing terrorist attacks. *See*, *e.g.*, 6 U.S.C. §§ 211(c)(5), (c)(9), (g)(3)(A)-(B), (g)(4)(C)(i); 8

C.F.R. § 235.1; 19 C.F.R. § 162.6; *Tabbaa v. Chertoff*, 509 F.3d 89, 97 (2d Cir. 2007) (describing antiterrorism mission of CBP and DHS).

a. The Terrorist Screening Dataset, the No Fly List, the Selectee List, and the Expanded Selectee List

The TSC maintains the Terrorist Screening Dataset ("TSDS"),[3] which is "the federal government's consolidated watchlist of known or suspected terrorists." *Elhady v. Kable*, 993 F.3d 208, 213 (4th Cir. 2021). Inclusion in the TSDS results from a multi-step assessment, based on analysis of available intelligence and investigative information about an individual. Exhibit 1, "Overview of the U.S. Government's Watchlisting Process and Procedures as of September 2020" ("Watchlisting Overview"), at 3.[4] The FBI receives, reviews, and forwards to the TSC "nominations" of individuals with a nexus to domestic terrorism for inclusion in the TSDS as known or suspected terrorists. *Id*. The National Counterterrorism Center, a component of the Office of the Director of National Intelligence, does the same for nominations of individuals with a nexus to international terrorism. *Id*. TSC then determines whether those nominations will be accepted. *Id*. For a known or suspected terrorist nomination to be accepted, it must include enough identifying information to allow screeners to determine whether the individual is a match to a record in the TSDS, and enough information to satisfy a reasonable suspicion that the individual is a known or suspected terrorist. *Id*.

The "reasonable suspicion" standard for inclusion in the TSDS is satisfied only where there exists "articulable intelligence or information which, based on the totality of the circumstances

[3] The TSDS was formerly known as the Terrorist Screening Database ("TSDB"). All references to the TSDB in case law would also be true of the TSDS.

[4] The Court may take judicial notice of this public document, as well as Defendants' other exhibits, which are integral to the Complaint. *See*, *e.g.*, *Zak v. Chelsea Therapeutics Int'l, Ltd.,* 780 F.3d 597, 607 (4th Cir. 2015).

and, taken together with rational inferences from those facts, creates a reasonable suspicion that the individual is engaged, has been engaged, or intends to engage, in conduct constituting[,] in preparation for, in aid or in furtherance of, or related to, terrorism and/or terrorist activities." *Id.* at 4. Mere guesses, hunches, or the reporting of suspicious activity alone are not sufficient to establish reasonable suspicion. *Id*. Nor can inclusion in the TSDS be based solely on an individual's race, ethnicity, or religious affiliation, nor solely on beliefs or activities protected by the First Amendment. *Id*.

The TSDS contains subsets of data, known as the No Fly List, the Selectee List, and the Expanded Selectee List. Inclusion on any of these lists requires satisfaction of additional criteria distinct from, and over and above, that which is required for designation as a known or suspected terrorist and inclusion in the TSDS generally. *Id*. The Government does not publicly disclose whether an individual is in the TSDS. Such status is protected by the law enforcement privilege, and the identities of those on the No Fly, Selectee, and Expanded Selectee lists are also statutorily protected as Sensitive Security Information ("SSI") pursuant to 49 U.S.C. § 114(r). *See, e.g.*, *Blitz v. Napolitano*, 700 F.3d 733, 737 n.5 (4th Cir. 2012); *Scherfen v. U.S. DHS*, No. 3:CV-08-1554, 2010 WL 456784, at *8 n.5 (M.D. Pa. Feb. 2, 2010); *see also* 49 C.F.R. § 1520.5(b)(9)(ii) (SSI includes "[i]nformation and sources of information used by a passenger or property screening program or system, including an automated screening system").

b. CBP's 2018 Directive on Border Searches of Electronic Devices

In January 2018, CBP issued a comprehensive Directive on Border Searches of Electronic Devices. *See* CBP Directive No. 3340-049A, "Border Searches of Electronic Devices" ("Electronic Device Policy"), Exhibit 2; *see also* Privacy Impact Assessment Update for CPB Border Searches of Electronic Devices, DHS/CBP/PIA-008(a) ("Privacy Impact Assessment"), Exhibit 3. Despite the "plenary authority of the Federal Government to conduct searches and

inspections of persons and merchandise crossing our nation's borders," CBP determined, "as a policy matter," to "impose[] certain requirements, above and beyond prevailing constitutional and legal requirements, to ensure that the authority for border searches of electronic devices is exercised judiciously, responsibly, and consistent with the public trust." Electronic Device Policy ¶ 4. Specifically, the Electronic Device Policy distinguishes between "basic" and "advanced" searches of electronic devices, and outlines the different procedures for each. *Id*. ¶¶ 5.1.3, 5.1.4. During a basic search, an "officer may examine an electronic device and may review and analyze information encountered at the border," with or without suspicion. *Id*. ¶ 5.1.3. Such searches "may reveal information that is resident upon the device and would ordinarily be visible by scrolling through the phone manually (including contact lists, call logs, calendar entries, text messages, pictures, videos, and audio files)." Privacy Impact Assessment at 6. "Following a basic search, if CBP is satisfied that no further information is needed, the electronic device is returned to the traveler and he or she is free to proceed." *Id*.

An advanced search occurs where an officer "connects external equipment" to a device so as to "review, copy, and/or analyze" its contents. Electronic Device Policy ¶ 5.1.4. CBP personnel are permitted to conduct such searches only where there is a "reasonable suspicion of activity in violation of the laws enforced or administered by CBP, or in which there is a national security concern, and with supervisory approval." *Id*. The Policy notes that "many factors may create reasonable suspicion or constitute a national security concern," including, for example, the "existence of a relevant national security-related lookout in combination with other articulable factors as appropriate, or the presence of an individual on a government-operated and government-vetted watch list." *Id*. For both basic and advanced searches, "[t]he border search will include an examination of only the information that is resident upon the device and accessible through the

device's operating system or through other software, tools, or applications." *Id.* ¶ 5.1.2.

Because it is not always possible to complete the search of a traveler's electronic device while he or she waits at the border, CBP Officers are permitted, with supervisory approval, to detain an electronic device beyond the "individual's departure from the port or other location of detention." *Id.* ¶ 5.4.1.1. "The search may take place on-site or at an off-site location, and is to be completed as expeditiously as possible"—in the absence of extenuating circumstances, generally no longer than five days. *Id.* ¶ 5.4.1. Extensions of detentions longer than five days must be approved by certain officials, while detentions longer than 15 days must be approved by other, higher-level officials, and such detentions may be approved and re-approved in increments of no longer than seven days. *Id.* ¶ 5.4.1.1.

The Electronic Device Policy also describes the standards regarding seizure and retention of an electronic device or information from the device. *See generally id.* ¶ 5.4.1. Without probable cause to seize an electronic device or a copy of the information contained therein, CBP "may retain only information relating to immigration, customs, and other enforcement matters if such retention is consistent with [an] applicable [Privacy Act] system[s] of records notice." *Id.* ¶ 5.5.1.2.

II. Plaintiff's Factual Allegations

Plaintiff alleges that he frequently travels both internationally and within the United States in connection with his business activities. Compl. ¶ 75. He speculates that he has been the target of "increased scrutiny at airports and border crossings" following an incident in September 2008 when his Somali-based company, while providing logistical support to a United Nations relief program in Somalia, came under attack by insurgent groups. *Id.* ¶¶ 77-80. After not traveling to the United States between approximately 2010 and 2018, *id.* ¶ 81, Plaintiff resumed travel to the United States in 2018 and alleges that "[f]ollowing every flight into the United States since 2018,"

id. ¶ 83, he has had his electronic devices seized by "Unknown CBP Officers," who then demanded his passwords. *Id*. He claims that the officers copied, uploaded and downloaded the data on his devices before releasing him with the devices and permitting him to enter the United States. *Id.* Plaintiff alleges that since 2020, he has refused to give officers the passwords to his devices, and that "[i]n some instances" officers would then seize his devices, "refusing to return them until an extended" search was conducted "offsite." *Id*. ¶ 84. He also alleges that he has been detained for several hours for questioning after returning to the United States. *Id*. ¶¶ 85, 87, 91.

III. Present Litigation

On February 17, 2022, Plaintiff filed this lawsuit against the CBP, FBI, and "unknown CBP officers" in their individual capacity. He brings four claims. First, in Count I, he alleges that CBP and FBI violated the Fourth Amendment rights of himself and "similarly situated Americans" by conducting secondary inspections and searching the electronic devices of those on "the federal watchlist." *See* Compl. ¶¶ 97-119. Second, in Count II, he alleges that the CBP and FBI violated his Fifth Amendment right against self-incrimination because CBP officers required him to provide the password to his electronic devices and to use facial recognition or fingerprints to open those devices. *See id*. ¶¶ 120-27. Third, in Count III, he alleges that the Government's "policies of searching and seizing Plaintiff and other United States citizens and permanent residents on the federal watchlist, as well as searching and seizing their cell phones," are arbitrary, capricious, an abuse of discretion, and unlawful. *See id*. ¶¶ 128-32. Finally, in Count IV, he brings a claim for damages against the unnamed officers under *Bivens*. *See id.* ¶¶ 133-37.

Plaintiff seeks injunctive and declaratory relief aimed at the Government's watchlisting and border search policies as a whole. S*ee id*. ¶¶ 138-40. Specifically, the relief requested includes an injunction prohibiting Defendants from applying "CBP Policy" that permits "nonroutine

detention and interrogation" of individuals and "forensic search[es]" of their electronic devices "solely because of watchlist status"; prohibiting Defendants from "ordering individuals at the border [to] provide passwords or biometric means to access electronic devices"; ordering Defendants to remove Plaintiff's purported watchlisting status; and ordering Defendants to "expunge any information illegally seized from" him. *Id.* ¶ 141. Plaintiff also requests a "declaratory judgment that Defendants placed [him] on the watchlist illegally." *Id.* ¶ 140.

STANDARD OF REVIEW

A motion under Federal Rule 12(b)(6) focuses "on the legal sufficiency of the complaint." *Giarratano v. Johnson*, 521 F.3d 298, 302 (4th Cir. 2008). A court will therefore "take the facts in the light most favorable to the plaintiff," but "need not accept the legal conclusions drawn from the facts," and "need not accept as true unwarranted inferences, unreasonable conclusions, or arguments." *E. Shore Mkts., Inc. v. J.D. Assocs. Ltd. P'ship*, 213 F.3d 175, 180 (4th Cir. 2000); *see also Bass v. E.I. DuPont de Nemours & Co.*, 324 F.3d 761, 765 (4th Cir. 2003). "To survive a motion to dismiss, a complaint must contain sufficient factual matter, accepted as true, to 'state a claim to relief that is plausible on its face.'" *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (quoting *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007)).

ARGUMENT

I. Plaintiff Fails To State a Claim Under the Fourth Amendment.

Plaintiff is not clear on whether he brings a facial or as-applied claim under the Fourth Amendment. Despite only offering facts describing a handful of interactions between himself and CBP officers, Plaintiff attempts to challenge CBP policy writ large, invoking the interests of "similarly situated" individuals. *See, e.g.*, Compl. ¶ 111 ("Defendants violated the rights of Plaintiff and similarly situated American citizens, permanent residents, and foreign nationals"); *id.* ¶ 112-19. Further, he seeks a sweeping injunction that "[p]rohibits Defendants from applying CBP

Policy that permits a forensic search of the electronic devices of US citizens or permanent residents" and that "permits nonroutine detention and interrogation of US citizens or permanent residents solely because of watchlist status." *Id*. ¶ 141. Plaintiff "seek[s] a remedy that far transcends any individual . . . plight." *Elhady*, 993 F.3d at 217; s*ee also Edgar v. Haines*, 2 F.4th 298, 313 (4th Cir. 2021) (explaining that a plaintiff brings a facial challenge when his "claim is that the policies and regulations are unconstitutional not as applied to their own conduct, but rather, *on their face*, as they apply to the population generally").[5]

Regardless of whether Plaintiff has brought a facial or an as-applied claim, his Fourth Amendment challenge fails. He has not plausibly alleged that CBP officers act pursuant to any "policy" beyond what is authorized by the express language of the Electronic Device Policy—the only CBP policy actually cited in the Complaint. Plaintiff repeatedly contends, *inter alia*, that that CBP policy mandates automatic forensic searches of TSDS listees' devices, but this fabricated "policy" has no basis in the Electronic Device Policy or even in his factual allegations.

To the extent Plaintiff facially challenges the Electronic Device Policy, rather than the factually unsupported "policies" appearing in his pleading, Plaintiff fails to show that that policy is unconstitutional in all of its applications, as he must in order to bring a facial challenge. *See City of L.A. v. Patel*, 576 U.S. 409, 415 (2015).

As-applied, Plaintiff's Fourth Amendment claim also fails. Any enhanced screening that Plaintiff underwent at the border is a routine search that does not require any suspicion. *See Tabbaa*, 509 F.3d at 98-99. Any manual searches of Plaintiff's electronic devices, *see* Compl. ¶¶

[5] Plaintiff also has not brought a putative class action, and he cannot litigate the rights of others who are not before the court. *See Gunnells v. Healthplan Servs., Inc.,* 348 F.3d 417, 458 (4th Cir. 2003) (noting that a "class action is an exception to the usual rule that litigation is conducted by and on behalf of the individual named parties only").

83, 85, 86, 87, are also routine searches that CBP officers may conduct without any suspicion at all. *See United States v. Ickes*, 393 F.3d 501, 502-03 (4th Cir. 2005). And Plaintiff has not plausibly alleged facts establishing that CBP officers lacked (or, in the future, will lack) reasonable suspicion to conduct an alleged "forensic search" of his devices—a standard similar to that required by the Electronic Device Policy itself. Accordingly, this Court should dismiss Plaintiff's Fourth Amendment claim.

a. Plaintiff Has Not Plausibly Alleged the Existence of CBP "Policies" Beyond the Electronic Device Policy.

Plaintiff purports to challenge numerous "policies and practices," but he does not plausibly allege that these policies actually exist. He first refers to an "official policy and practice" pursuant to which CBP, without exception, "refers TSDS listees to secondary inspection," Compl. ¶¶ 68, 99. But he identifies no CBP policy instructing officers to refer TSDS listees to secondary inspection in the uniform matter Plaintiff suggests.

He then makes allegations concerning electronic device searches, *see id.* ¶¶ 100-04, 109-18, which are governed by CBP's Electronic Device Policy. But Plaintiff's unsupported factual allegations bear scant relation to what the Electronic Device Policy actually says. *See, e.g.*, *id.* ¶¶ 69-70. Nowhere in the Electronic Device Policy, for example, does it require that CBP officers compel alleged listees to "provide biometric fingerprints to determine whether they are in the TSDB." *Id.* ¶ 99. Nor does the policy *require* that CBP officers automatically conduct forensic searches of the electronic devices of TSDS listees, contrary to Plaintiff's numerous assertions. *See, e.g.*, *id.* ¶ 7 (CBP officers "saw [Plaintiff's] status" and "did what those conclusory labels told them to do"); ¶ 70 ("CBP officers are directed to conduct an advanced forensic search of any electronics carried by TSDB listees"); *id.* ¶ 72 ("CBP officers are directed to . . . conduct a nonroutine forensic search and seizure of all electronics" of TSDS listees); *id.* ¶ 100 ("[A]s a matter

of official policy and practice, Defendants . . . conduct a forensic search of the contents of the electronic devices of individuals on the TSDB"). Rather, the Policy states that an Officer "*may* perform an advanced search" when "there is reasonable suspicion of activity in violation of the laws enforced or administered by CBP, or in which there is a national security concern, and with supervisory approval." Electronic Device Policy ¶ 5.1.4. Plaintiff also asserts that "CBP officers are directed to disregard factors for and against a search and seizure of electronic devices in the possession of TSDB listees," Compl. ¶ 72, but again, nothing in the Policy directs officers to do so. And the Complaint itself belies Plaintiff's would-be characterization of these policies: in one encounter with CBP, Plaintiff does not allege that officers searched his phone at all (let alone forensically searched it). *See id*. ¶ 89.

The "policies" Plaintiff purports to challenge, therefore, are each a straw man. Plaintiff would have the Court believe that CBP has instituted a series of shadow policies that deviate from its actual, written policies. But Plaintiff merely alleges that Defendants "took certain action with respect to [him] and asks the Court to surmise therefrom the existence of a broader policy"—and that is "not enough" to plausibly allege that such a policy exists. *Pearl River Union Free Sch. Dist. v. King*, 214 F. Supp. 3d 241, 260 (S.D.N.Y. 2016); *see also Al Otro Lado, Inc. v. Nielsen*, 327 F. Supp. 3d 1284, 1320 (S.D. Cal. 2018) (holding the plaintiff's "disparate 'examples'" of conduct by CBP officials does not support "the inference that there is an overarching policy"). Rather than allege facts showing that such straw man policies exist, Plaintiff makes bare assertions without any support. *See, e.g.*, *id*. ¶ 115 (challenging "Defendants' policies requiring CBP officers . . . to conduct a nonroutine forensic search of Plaintiff's electronic devices and the electronic devices of similarly situated Americans"). These assertions do not suffice. *Iqbal*, 556 U.S. at 678 (holding that the plaintiff's bare allegations of a "policy" of harsh conditions of confinement and

widespread detention based on race did not plausibly state a claim); *cf. Bark v. U.S. Forest Serv.*, 37 F. Supp. 3d 41, 50 (D.D.C. 2014) (holding the plaintiffs could not challenge alleged unwritten Forest Service "policies" because they "point[ed] to no written rules, orders, or even guidance documents of the Forest Service that set forth the supposed policies challenged"); *Lujan v. Nat'l Wildlife Fed'n*, 497 U.S. 871, 875 (1990) (holding that the plaintiffs could not broadly challenge a "land withdrawal review program" instead of challenging discrete government actions). Accordingly, to the extent Plaintiff challenges any "policies" that go beyond the scope of the express terms of the Electronic Device Policy, Plaintiff has failed to state a claim and such challenges should be dismissed.

b. Plaintiff Has Failed to Adequately Plead a Facial Claim Challenging the Electronic Device Policy.

Facial claims are "the most difficult challenge to mount successfully, since the challenger must establish that no set of circumstances exists under which the Act would be valid," *Salerno*, 481 U.S. at 745, meaning the law or policy in question "lacks any 'plainly legitimate sweep,'" *United States v. Stevens,* 559 U.S. 460, 472 (2010) (quoting *Washington v. Glucksberg,* 521 U.S. 702, 740 n.7 (1997)). The fact that the challenged law or policy "might operate unconstitutionally under some conceivable set of circumstances is insufficient to render it wholly invalid." *Id.; see also Elhady*, 993 F.3d at 217 ("When considering a facial challenge such as this one, we note that programs can withstand such facial attacks whenever they are capable of constitutional applications."). While "facial challenges under the Fourth Amendment are not categorically barred," *Patel*, 576 U.S. at 415, such challenges can only succeed where a law is "unconstitutional in all of its applications" and the "proper focus of the constitutional inquiry is searches that the law actually authorizes," *id.* at 418 (citation omitted).

When stripped of Plaintiff's unsupported surplusage, CBP's policies easily survive scrutiny against a facial challenge. Under the Fourth Amendment, "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated …" U.S. Const. amend. IV. "[T]he ultimate touchstone of the Fourth Amendment is 'reasonableness,'" *Brigham City v. Stuart*, 547 U.S. 398, 403 (2006), which "ordinarily . . . requires the obtaining of a judicial warrant," *Riley v. California*, 573 U.S. 373, 381-82 (2014) (citation omitted). However, there are several important exceptions to this rule, including one that "covers our nation's borders." *United States v. Kolsuz*, 890 F.3d 133, 137 (4th Cir. 2018).

Under the border search exception, CBP has the authority to conduct routine searches and seizures at the border without "any requirement of reasonable suspicion, probable cause, or warrant." *United States v. Montoya de Hernandez*, 473 U.S. 531, 537 (1985). "[S]earches made at the border, pursuant to the longstanding right of the sovereign to protect itself by stopping and examining persons and property crossing into this country, are reasonable simply by virtue of the fact that they occur at the border." *United States v. Flores-Montano*, 541 U.S. 149, 152-53 (2004) (citation omitted); *see also United States v. Ramsey*, 431 U.S. 606, 619 (1977) ("The "longstanding recognition that searches at our borders without probable cause and without a warrant are nonetheless 'reasonable' has a history as old as the Fourth Amendment itself."). While the Supreme Court has recognized a small subset of "highly intrusive" border searches that are considered "nonroutine" and require some level of individualized suspicion, *Flores-Montano*, 541 U.S. at 152, generally speaking, "the Fourth Amendment balance between the interests of the Government and the privacy right[s] of the individual is [ ] struck much more favorably to the Government." *Montoya de Hernandez,* 473 U.S. at 540.

As explained in Part I.a., *supra*, Plaintiff has failed to plausibly allege the existence of the vast majority of the purported "policies" that he challenges. But to the extent Plaintiff seeks to bring a facial challenge to the Electronic Device Policy—and in particular, its provision permitting officers to conduct advanced searches when an officer has reasonable suspicion of unlawful activity or a national security concern, *see* Electronic Device Policy ¶ 5.1.4—this claim fails because Plaintiff has not shown that the Policy is "unconstitutional in all of its applications." *Patel*, 576 U.S. at 418.

The First Circuit recently upheld the constitutionality of the Electronic Device Policy. *Alasaad v. Mayorkas*, 988 F.3d 8, 12 (1st Cir. 2021) ("[W]e conclude that the challenged border search policies, both on their face and as applied to the two plaintiffs who were subject to these policies, are within permissible constitutional grounds."), *cert. denied*, *Merchant v. Mayorkas*, 141 S. Ct. 2858 (2021). And the Policy reflects existing law in the Fourth Circuit, which held that a "*forensic* search of [] cell-phone data qualifies as a nonroutine border search, requiring *some level of particularized suspicion*." *Kolsuz*, 890 F.3d at 144 (emphasis added).[6] The Electronic Device Policy, similarly, states that a CBP officer may only conduct an "advanced search"—or "any search in which an Officer connects external equipment, through a wired or wireless connection, to an electronic device not merely to gain access to the device, but to review, copy, and/or analyze its contents"—when "there is reasonable suspicion of activity in violation of the laws enforced or

[6] Because the Government had reasonable suspicion for the search in *Kolsuz* and because an "established and uniform body of precedent" permits warrantless border searches of devices with reasonable suspicion, *Kolsuz* did not reach the issue of whether "some level of particularized suspicion" requires reasonable suspicion or something "more." 890 F.3d at 144, 148. Further, Defendants respectfully disagree with *Kolsuz*'s conclusion that individualized suspicion is required for forensic searches of devices at the border, a conclusion in conflict with another recent Circuit Court decision. *See United States v. Touset*, 890 F.3d 1227, 1233 (11th Cir. 2018) ("We see no reason why the Fourth Amendment would require suspicion for a forensic search of an electronic device when it imposes no such requirement for a search of other personal property.").

administered by CBP, or in which there is a national security concern, and with supervisory approval at Grade 14 or higher." Electronic Device Policy ¶ 5.1.4. Accordingly, before conducting a forensic search, CBP policy requires either reasonable suspicion or a national security concern. *See Kolsuz*, 890 F.3d at 137 (the forensic examination of Kolsuz's phone requires "some measure of individualized suspicion").

Plaintiff appears to contend that the Policy violates the Fourth Amendment because it states that, while "[m]any factors may create reasonable suspicion or constitute a national security concern," one example includes "the presence of an individual on a government-operated and government-vetted terrorist watchlist." Electronic Device Policy ¶ 5.1.4; *see also* Compl. ¶ 114 (alleging that the Fourth Amendment rights of Plaintiff and similarly situated individuals are violated by "CBP's policy that the presence of an individual on a 'government operated and government vetted terrorist watch list' alone constitutes grounds" for CBP to forensically search electronic devices). But Plaintiff has not demonstrated that "no set of circumstances exists under which the [Policy] would be valid." *Salerno*, 481 U.S. at 745. He only offers facts concerning eight interactions he alone had with CBP, *see* Compl. ¶¶ 83-96, not border crossing incidents involving any other "similarly situated" individual, much less any individual confirmed to be on the TSDS.

Plaintiff's facial challenge is therefore self-defeating. Even if Plaintiff argues that some TSDS designations—or even his alleged designation—have resulted from insufficient information, this does not render the Electronic Device Policy facially invalid. He does not claim that the Government never has reasonable suspicion to place someone on a watchlist, and accordingly, to conduct a forensic search of his or her devices if circumstances warrant. *See Kolsuz*, 890 F.3d at 144. Nor could he. Indeed, the Government is generally *required* to have reasonable suspicion of terrorism-related activity to list someone on the TSDS. Watchlist Overview at 3-4.

Not even Plaintiff contends that no single person on the TSDS warrants his or her placement there. Plaintiff necessarily must concede that conducting forensic searches based on TSDS status would not, in every instance, "require officers to violate the Fourth Amendment." *Cottman v. Baltimore Police Department*, No. 21-CV-00837-SAG, 2022 WL 137735, at *4 (D. Md. Jan. 13, 2022).

Moreover, the Electronic Device Policy is permissive and does not "require officers to search or seize such property *in every relevant instance*." *Id*. (emphasis in original). It states that an officer "*may* perform an advanced search of an electronic device" when the requisite conditions are met. Electronic Device Policy ¶ 5.1.4 (emphasis added). As noted, *supra*, Plaintiff's own allegations confirm as much. Compl. ¶ 89 (allegation of inspection with no search of Plaintiff's electronic devices). Both by design and as Plaintiff's allegations reflect, in many instances, CBP officers will not conduct forensic searches of electronic devices of TSDS designees.

As the Fourth Circuit explained in *Elhady*—which rejected a facial challenge to watchlisting policies under the Fifth Amendment—the Fourth Amendment is an appropriate vehicle for bringing claims challenging law enforcement actions at airports or the border precisely because it allows courts to "conduct the kind of individualized case-by-case analyses that are precluded in a facial due process challenge." 993 F.3d at 224-25. That follows, the Court noted, from the fact that "adopting the most extreme allegations for a holding of facial invalidity would encourage facial attacks on all manner of programs and initiatives with all of their attendant anti-democratic consequences." *Id.* at 217. Since Plaintiff cannot show that conducting an advanced search of the devices of an individual on the TSDS would be unlawful in all instances, he has failed to "shoulder [the] heavy burden" required to bring a facial challenge to the Electronic Device Policy. *Salerno*, 481 U.S. at 745. Accordingly, this Court should dismiss any facial challenge under the Fourth Amendment.

c. Plaintiff Has Failed to Plead a Viable As-Applied Fourth Amendment Claim.

Plaintiff's as-applied Fourth Amendment challenge to his alleged searches and seizures also fails as a matter of law. Plaintiff seeks only prospective relief, attempting to use his eight prior encounters at the border as a basis for an injunction prohibiting Defendants from "applying CBP policy" that "permits a forensic search" of TSDS listees' electronic devices and from "applying CBP policy" that permits "nonroutine detention and interrogation" of TSDS listees. Compl. ¶ 141.a.-b. Plaintiff does not even appear to challenge the individual searches as unlawful—instead framing his challenge as one against policies, both actual and hypothetical. But however framed, CBP's conduct was lawful under the Fourth Amendment such that no future injunction is warranted.

First, Plaintiff's referrals to secondary inspection based on his alleged TSDS status,[7] *see* Compl. ¶¶ 85-93, would not violate the Fourth Amendment because CBP officers may conduct routine searches and seizures at the border without any suspicion. *See* Part I.b., *supra*. Second, even if CBP did conduct forensic searches of Plaintiff's electronic devices based solely on his purported TSDS status,[8] those searches were lawful because his alleged TSDS status gives rise to the "reasonable suspicion" required by the Fourth Amendment.

Secondary inspections are routine searches that do not require any heightened suspicion. They are far less invasive than other searches that have been deemed "routine," such as searching

[7] Defendants reiterate here that they assume the accuracy of this allegation for purposes of Rule 12 only, and neither confirm nor deny Plaintiff's actual status on or off the TSDS.

[8] In several instances, Plaintiff does not specify whether the officers conducted manual or forensic searches. *See, e.g.*, Compl. ¶ 85 (officers "took his electronic devices into another room after asking for and receiving the passwords"); *id*. ¶ 90 (officers "took his devices into another room"); *id*. ¶ 91 (officers "took his devices"). The Fourth Circuit has held that a non-forensic, or manual, search of a computer constitutes a routine search requiring no suspicion. *Ickes*, 393 F.3d at 505-06. Therefore, any alleged manual search of Plaintiff's electronic devices did not (and prospectively would not) violate the Fourth Amendment.

the inside of an automobile gas tank, *Flores-Montano*, 541 U.S. at 155, and a manual search of a laptop, *Ickes*, 393 F.3d at 502-03. And a secondary inspection does not resemble the searches other courts have found as "nonroutine," such as "strip, body cavity, or involuntary x-ray searches." *Montoya de Hernandez*, 473 U.S. at 541 n. 4. Even an inspection that is "more rigorous than many of the secondary inspections given to people who arouse suspicion when attempting to the enter the United States" is routine. *Tabbaa*, 509 F.3d at 98-99. Moreover, even if Defendants "compelled" TSDS listees to "provide biometric fingerprints," Compl. ¶ 99, such fingerprinting "does not take the searches out of the realm of what is considered routine because, at least in the context of a border search, being fingerprinted (even forcibly) . . . is not particularly invasive." *Tabbaa*, 509 F.3d at 99. Because these secondary inspections are routine, they do not require any reasonable suspicion at all. *See Ickes*, 393 F.3d at 505. Therefore, any CBP policy referring those listed on the TSDS to secondary inspection, either automatically (which CBP policy does not require), or as a matter of officer discretion (which CBP policy contemplates) plainly does not violate the Fourth Amendment, and Plaintiff's challenge to this aspect of CBP's conduct fails.

Plaintiff also alleges that CBP engaged in forensic searches of his electronic devices "solely because" he is "listed on the federal terrorist watchlist." Compl. ¶ 110. To the extent Plaintiff alleges that CBP policy dictates that his purported TSDS status automatically results in forensic searches of his electronics, he has not plausibly alleged that such a policy exists. *See* Part I.a., *supra*. As explained, the Electronic Device Policy permits advanced searches, but does not mandate them, *see* Electronic Device Policy ¶ 5.1.4 (officers "may" perform an advanced search when the circumstances permit), and Plaintiff's own allegations confirm this, *see* Compl. ¶ 89 (no allegation that his electronic devices were searched on June 30, 2020 entry).

To the extent Plaintiff alleges that the Policy permits TSDS status to serve as a basis for

conducting a forensic search in *some* instances, such a policy would not be constitutionally infirm.[9] TSDS status *does* provide the "individualized suspicion" required for a nonroutine search. *Kolsuz*, 890 F.3d at 144; *United States v. Saboonchi*, 990 F. Supp. 2d 536, 545 (D. Md. 2014) (observing that "reasonable suspicion" is required for a nonroutine search). Under the Fourth Amendment, "reasonable suspicion" means that under the "totality of the circumstances," there is "particularized and objective basis for *suspecting* legal wrongdoing." *United States v. Bernard*, 927 F.3d 799, 805 (4th Cir. 2019) (emphasis added); *see id*. (finding reasonable suspicion based solely on an officer's observation of erratic driving).

At the border, a reasonable suspicion inquiry "simply considers, after taking into account all the facts of a particular case, whether the border official ha[d] a reasonable basis on which to conduct the search." *United States v. Irving*, 452 F.3d 110, 124 (2d Cir. 2006) (citation omitted). "Reasonable suspicion is a relatively low standard and border officials are afforded deference due to their training and experience." *Abidor v. Napolitano*, 990 F. Supp. 2d 260, 282 (E.D.N.Y. 2013). CBP officers "are trained to assess a 'totality of circumstances' when making determinations on the appropriate actions to take during a border inspection." Privacy Impact Assessment at 5. One "example[]" of a factor to consider is presence on a government watchlist. *See* Electronic Device Policy ¶ 5.1.4.

Inclusion of a known or suspected terrorist on the TSDS must already satisfy a similar "reasonable suspicion" standard, in which there exists "articulable intelligence or information

[9] The Court need not decide this question. As noted, it is not entirely clear whether Plaintiff seeks an injunction against *automatic* future inspection based on alleged future TSDS status, or an injunction against *any* future inspection based on such status. Defendants construe Plaintiff's claims to seek the former. Plaintiff cannot obtain relief against automatic searches because neither CBP policy nor Plaintiff's individual allegations demonstrate that existing policy requires any kind of search based on TSDS status, let alone forensic device searches.

which, based on the totality of the circumstances and, taken together with rational inferences from those facts, creates a reasonable suspicion that the individual is engaged, has been engaged, or intends to engage, in conduct constituting[,] in preparation for, in aid or in furtherance of, or related to, terrorism and/or terrorist activities." Watchlisting Overview at 4. And CBP officers "may rely on information furnished by other law enforcement officials to establish reasonable suspicion." *Albright v. Rodriguez*, 51 F.3d 1531, 1536 (10th Cir. 1995); *see also Karadi v. Jenkins*, 7 F. App'x 185, 192 (4th Cir. 2001) ("An officer may rely on information provided by a known third party to establish a reasonable suspicion that could justify an investigatory stop."). Moreover, *Kolsuz* itself favorably cited CBP's Electronic Device Policy, noting with approval that under the policy, advanced searches "may be conducted only with reasonable suspicion of activity that violates the customs laws or in cases raising national security concerns." 890 F.3d at 146 (citing the Electronic Device Policy).

The border search exception's underlying principles underscore why individuals who the Government reasonably suspects to be known or suspected terrorists would satisfy the threshold to conduct a more invasive electronic device search. At "our nation's borders," the Supreme Court "has long recognized the federal government's substantial sovereign interests in protecting territorial integrity and national security." *United States v. Aigbekaen*, 943 F.3d 713, 720 (4th Cir. 2019) (citation omitted). It is "axiomatic that the United States, as sovereign, has the inherent authority to protect, and a paramount interest in protecting, its territorial integrity." *Ickes*, 393 F.3d at 506 (citing *Flores-Montano*, 541 U.S. at 153). At the border, customs officials "have more than merely an investigative law enforcement role"; they "are also charged, along with immigration officials, with protecting this Nation from entrants who may bring anything harmful into this country, whether that be communicable diseases, narcotics, or explosives." *Montoya de*

Hernandez, 473 U.S. at 544. Protecting the sovereign from foreign terror threats falls squarely within this role. Searching for potential information that may implicate national security threats "is vital to achieving the border search exception's purposes of controlling 'who and what may enter the country.'" *Alasaad*, 988 F.3d at 20 (citing *Ramsey*, 431 U.S. at 620). The government's interest in "preventing the entry of unwanted persons and effects is at its zenith at the international border." *Flores-Montano*, 541 U.S. at 152. As such, assuming *arguendo* that Plaintiff was on the TSDS, the CBP officer had a reasonable basis on which to conduct the search. And importantly, since Plaintiff's claims are prospective, if Plaintiff were on the TSDS in the future, such status would provide sufficient suspicion to warrant inspection, if an officer chose to undertake such an inspection.[10]

II. Plaintiff Fails To State a Claim Under the Fifth Amendment.

Plaintiff next brings a claim under the Fifth Amendment, alleging that Defendants violate his right against self-incrimination by forcing him to provide passwords and to use his fingerprints and facial recognition so they could access his electronic devices at the border. Compl. ¶ 124. The Fifth Amendment's Self-Incrimination Clause provides that "[n]o person . . . shall be compelled in any criminal case to be a witness against himself." U.S. Const. amend. V. The right against self-incrimination "applies only when the accused is compelled [1] to make a testimonial communication [2] that is incriminating." *United States v. Sweets*, 526 F.3d 122, 127 (4th Cir. 2007) (citation omitted). Plaintiff's Fifth Amendment claim fails for several reasons.

First, the right against self-incrimination only applies when introduced against a criminal defendant at trial, not in civil cases such as this one. This is evident from the text of the Clause,

[10] If the Court determines that the as-applied claim against CBP cannot be resolved without assessing the particular merits of any alleged TSDS placement, only such an individualized claim concerning Plaintiff alone—not policy-based facial challenges—would remain.

which protects an individual from being "compelled *in any criminal case* to be a witness against himself." U.S. Const. amend. V (emphasis added). Moreover, the Supreme Court has held that the Fifth Amendment right against self-incrimination is a "fundamental trial right of criminal defendants" and accordingly, a violation of such a right "only occurs at trial." *United States v. Verdugo-Urquidez*, 494 U.S. 259, 264 (1990). The Supreme Court's decision in *Chavez v. Martinez* is instructive. In *Chavez*, a civil 42 U.S.C. § 1983 case, the plaintiff, Martinez, alleged that officers who coercively questioned him violated his right against self-incrimination. *Chavez*, 538 U.S. at 765. The plurality opinion rejected this claim, explaining that "[w]e fail to see how, based on the text of the Fifth Amendment, Martinez can allege a violation of this right, since Martinez was never prosecuted for a crime, let alone compelled to be a witness against himself in a criminal case." *Id.* at 766. The Fourth Circuit has also repeatedly adhered to this rule. *See, e.g.*, *United States v. Riley*, 920 F.3d 200, 205 (4th Cir. 2019) (holding that "the Self-Incrimination Clause is violated *only* if those statements are used in a criminal trial"); *United States v. Oloyede*, 933 F.3d 302, 310 (4th Cir. 2019) (no Fifth Amendment violation where the case "the admission into evidence of data" from a phone "present[ed] no risk that ... *coerced statements* (however defined) [would] be used against [her] at a criminal trial."); *Riley v. Dorton*, 115 F.3d 1159, 1164 (4th Cir. 1997), *abrogated other grounds by Wilkins v. Gaddy*, 559 U.S. 34 (2010) ("following the plain text of the Amendment . . . most courts refuse to find a Fifth Amendment violation even where statements were made, but were not actually used in a criminal proceeding").[11] Similarly, Plaintiff brings a civil action and does not allege that he is being prosecuted for any crime. *See Chavez*, 538 U.S. at 766.

[11] To the extent that the district court in *El Ali v. Barr*, 473 F. Supp. 3d 479 (D. Md. 2020), held that certain plaintiffs had stated a self-incrimination claim based on coercive interviews and

The only occasion in which the Fifth Amendment's self-incrimination privilege can be asserted in noncriminal cases is "where the answers might incriminate [the suspect] in *future criminal proceedings*." *Id*. at 770 (citation omitted). In determining whether future prosecution is likely, "the proper test simply assesses the objective reasonableness of the target's claimed apprehension of prosecution." *United States v. Sharp*, 920 F.2d 1167, 1171 (4th Cir. 1990). Here, Plaintiff alleges no facts suggesting a reasonable apprehension that he would be subject to criminal process. Plaintiff himself acknowledges that he has "never been charged" with a crime and he "is not under investigation." Compl. ¶ 3. Nor can he ground his claim on mere speculation that his information may be used against him in some hypothetical future prosecution. *See Zicarelli v. New Jersey State Comm'n of Investigation*, 406 U.S. 472, 478 (1972) ("It is well established that the privilege [against self-incrimination] protects against real dangers, not remote and speculative possibilities."); *Sharp*, 920 F.2d at 1170 (explaining that the right against self-incrimination cannot be invoked by claiming only that the information "sought by the government *may* be incriminating") (emphasis added); c*f. United States v. (Under Seal)*, 794 F.2d 920, 924 (4th Cir. 1986) (noting, in the context of fear of prosecution by foreign sovereign as a basis for invoking Fifth Amendment privilege, the "fear of prosecution [must be] real and substantial, rather than speculative and remote").

Moreover, even if Plaintiff's interactions with CBP were coercive, this cannot serve as a proxy for fear of future criminal prosecution. The "mere use of compulsive questioning, without more," does not violate the Constitution. *Chavez*, 538 U.S. at 767. CBP officials conducted these

---

searches of electronic devices during border inspections, that court's analysis was misplaced. The court rested its conclusion on whether "Plaintiffs [] averred sufficient facts to make plausible the claim that their will had been overborne during their interrogations," *id.* at 522, and ignored the law requiring that the information be used in a criminal proceeding.

interviews pursuant to established policies and procedures under CBP's statutory and regulatory authority, which undermines any suggestion of potential criminal prosecution. *See Baltimore City Dep't of Soc. Servs. v. Bouknight*, 493 U.S. 549, 556 (1990) ("The Court has on several occasions recognized that the Fifth Amendment privilege may not be invoked to resist compliance with a regulatory regime constructed to effect the [government's] public purposes unrelated to the enforcement of its criminal laws."); *United States v. Ka*, 982 F.3d 219, 222 (4th Cir. 2020) (Self-Incrimination Clause not applicable in supervised release revocation proceedings since such proceedings "are not part of the underlying criminal prosecution").

Because Plaintiff has not alleged that any statements made to CBP officers are being used in a criminal proceeding against him nor that he has any reasonable fear of future prosecution, he has failed to state a claim under the Self-Incrimination Clause. Count II should be dismissed on this basis alone. *See Majid v. Cnty. of Montgomery, Maryland*, No. CV TDC-20-1517, 2021 WL 4441349, at *4 (D. Md. Sept. 28, 2021) (rejecting a civil plaintiff's Fifth Amendment self-incrimination claims because he "has not alleged that any statement" he made to an officer "has been used against him in a criminal case").

Second, Plaintiff has not alleged that his devices contained any incriminating material obtained by law enforcement during any one of the incidents referenced in his complaint. *See Sharp*, 920 F.2d at 1170 (noting that the first question is "whether the information is incriminating in nature."). Here, Plaintiff has only alleged in conclusory fashion that he was forced to provide biometric information so that officers could access his electronic devices during a border search. But he has not alleged anything about the content of that information, much less that it would incriminate him in a future criminal case. He has not demonstrated that any initial refusal to provide his device access information to CBP agents was "based on any articulated real and

appreciable fear that [the information] would be used to incriminate him, or that it 'would furnish a link in the chain of evidence needed to prosecute' him." *Hiibel v. Sixth Jud. Dist. Ct. of Nevada, Humboldt Cnty.,* 542 U.S. 177, 190 (2004) (quoting *Hoffman v. United States,* 341 U.S. 479, 486 (1951)). He alleges that his "data" was "searched," "copied," and "downloaded," *see, e.g.,* Compl. ¶¶ 83, 86, but gives no detail about what that data contains. In other instances, he alleges that he refused to answer any questions at all. *Id*. ¶ 91-92. "Courts have not found Fifth Amendment violations where no statements whatsoever were made." *Riley*, 115 F.3d at 1164.

Third, even if this claim were adequately pled, the appropriate remedy is not a civil injunction or declaratory relief of the type sought here, but rather it is exclusion of evidence in subsequent criminal proceedings. *See Antonio v. Moore*, 174 F. App'x 131, 135 n. 2 (4th Cir. 2006) (noting that "the complete and sufficient remedy for a perceived" Fifth Amendment "violation is the exclusion of such statements at trial"); *United States v. Cavin*, 553 F.2d 871, 873 (4th Cir. 1977) (the remedy for a violation of the Self-Incrimination Clause is "circumscribed" and is "suppression of his statement"); *see also Chavez*, 538 U.S. at 777 (Souter, J., concurring) ("the core of the guarantee against compelled self-incrimination is the exclusion of any such evidence.").

This clear precedent also applies to Plaintiff's claim seeking expungement of the information that CBP agents allegedly gathered from Plaintiff, Compl. ¶ 141(d). Expungement "is a relief confined to exceptional circumstances." *Allen v. Webster*, 742 F.2d 153, 155 (4th Cir. 1984). Indeed, a district court considering similar Fourth Amendment claims declined to order expungement of the information gathered during an electronic device search because "[e]ven where evidence obtained in an unconstitutional manner has been suppressed, a further remedy of

expungement does not follow." *Alasaad v. Nielsen*, 419 F. Supp. 3d 142, 172 (D. Mass. 2019).[12]

Fourth, Plaintiff's claim fails on the independent ground that the border search doctrine permits the Government to require that electronic devices, like all other merchandise and cargo, be presented to customs officials in a manner that allows for their inspection. Whether Defendants may lawfully search Plaintiff's electronic devices is a separate inquiry, discussed at length above. *See* Part I, *supra*. But because customs officials have clear authority to search a traveler's cargo, "no matter how great the traveler's desire to conceal the contents may be," *United States v. Ross*, 456 U.S. 798, 823 (1982), it follows that CBP may lawfully require the traveler to present the cargo in a manner in which it may be inspected. For example, if a traveler arrives with a locked container or suitcase, CBP may lawfully require him to unlock the container—and, in the event that he refuses, CBP is permitted to take action to remove the lock, and is by no means required to permit the entry of the cargo into the United States until it has ascertained the contents of the container. *See*, *e.g.*, 19 U.S.C. §§ 1461, 1462, 1496, 1499, 1582; 6 U.S.C. § 211(k). In practical terms, "[a] password is simply a digital lock," directly analogous to the locks "present on luggage and briefcases," which "are subject to 'routine' searches at ports of entry all the time." *United States v. McAuley*, 563 F. Supp. 2d 672, 678 (W.D. Tex. 2008); *see also Saboonchi*, 990 F. Supp. 2d at 560-61. There is no reason why any different result should obtain—regardless of whether the cargo in question is a physical container or an electronic device—simply because a particular lock is in electronic form. Given that at the border, the "Government's interest in preventing the entry of unwanted persons and effects is at its zenith," *Flores-Montano*, 541 U.S. at 152, it would be

[12] The District Court in *Alasaad* declined to order expungement even after finding constitutional violations—a holding later reversed by the First Circuit. *See Alasaad v. Mayorkas*, 988 F.3d 8, 13 (1st Cir. 2021) (holding that advanced searches of devices at the border do not require a warrant or probable cause, that basic searches of devices are routine and that may be performed without reasonable suspicion).

absurd to recognize a Fifth Amendment violation for the unlocking of a cell phone when that action is permitted by the Fourth Amendment's border search exception. For these reasons, Plaintiff fails to state a self-incrimination claim under the Fifth Amendment, and this claim should be dismissed.

III. Plaintiff's APA Claim Should Be Dismissed.

Plaintiff's APA claim should also be dismissed. *First*, any such claim is coextensive with his constitutional claims, and should be analyzed as such (and dismissed for the same reasons). *See Ass'n of Priv. Sector Colleges & Universities v. Duncan*, 681 F.3d 427, 442 (D.C. Cir. 2012) ("Where we conclude that a challenged regulatory provision does not exceed the [statutory] limits and otherwise satisfies the requirements of the APA, we will uphold the provision and preserve the right of complainants to bring as-applied challenges against any alleged unlawful applications."). He makes no new allegations, nor cites any authority for the proposition that the APA requires something more than what the Constitution does in this context. *See* Compl. ¶ 129. Moreover, apart from his (erroneous) claims that CBP's phantom "policy" of automatic referral of TSDB listees to electronic device searches violates the Constitution, he has not plausibly alleged other grounds that any agency action is "arbitrary and capricious," "an abuse of discretion," or "otherwise not in accordance with law." 5 U.S.C. § 706.

Second, the APA authorizes review only of final, discrete agency actions, *see* 5 U.S.C. § 704, and Plaintiff does not clearly identify the agency action he challenges. Instead, he speculates about the existence of some undefined government policy requiring CBP officers to forensically search the devices of TSDB listees. The APA "does not provide judicial review for everything done by an administrative agency." *Hearst Radio v. FCC*, 167 F.2d 225, 227 (D.C. Cir. 1948). Rather, the statute defines "agency action" to "include[] the whole or a part of an agency rule, order, license, sanction, relief, or the equivalent or denial thereof, or failure to act." 5 U.S.C. § 551(13). "All of those categories involve circumscribed, discrete agency actions, as their

definitions make clear." *Norton v. S. Utah Wilderness All.*, 542 U.S. 55, 62 (2004); *see also City of New York v. United States Dep't of Def.*, 913 F.3d 423, 431 (4th Cir. 2019) ("Courts are well-suited to reviewing specific agency decisions, such as rulemakings, orders, or denials," not "generalized grievances asking us to improve an agency's performance or operations."). As discussed in greater detail, *see* Part. I.a, *supra*, Plaintiff invents from whole-cloth CBP "policies" from which he claims ongoing injury. But the APA only permits challenges to "discrete" policies, not "all conduct on the part of the government." *City of New York,* 913 F.3d at 430. Because Plaintiff has not identified discrete agency action (and indeed has rested his claims on the existence of an undocumented, unsubstantiated shadow policy), his APA claim fails.

Third, even if he did identify a discrete agency action, Plaintiff's conclusory allegations do not meet the standard required to plausibly state an APA claim. "To survive a motion to dismiss, a complaint must contain sufficient factual matter, accepted as true, to state a claim to relief that is plausible on its face." *Iqbal*, 556 U.S. at 678 (citation omitted). In Count III, Plaintiff broadly asserts, without factual support, that Defendants' policies "are arbitrary and capricious, an abuse of discretion, and otherwise not in accordance with law, and should be set aside as unlawful pursuant to 5 U.S.C. § 706." Compl. ¶ 130. Plaintiff merely regurgitates the elements of an APA claim without any supporting facts. "Threadbare recitals of the elements of a cause of action, supported by mere conclusory statements do not suffice." *Iqbal*, 556 U.S. at 678. He points to no facts suggesting that, in enacting such phantom "policies," CBP "has relied on factors which Congress has not intended it to consider, entirely failed to consider an important aspect of the problem, offered an explanation for its decision that runs counter to the evidence before the agency, or is so implausible that it could not be ascribed to a difference in view or the product of agency

expertise." *Motor Vehicle Mfrs. Ass'n of U.S., Inc. v. State Farm Mut. Auto. Ins. Co.*, 463 U.S. 29, 43 (1983). Accordingly, he has failed to state an APA claim, and Count III should be dismissed.

IV. Any Challenge to Plaintiff's Alleged Watchlist Status Is Unsupported by the Complaint.

Finally, Plaintiff does not appear to challenge to his alleged placement on any government terrorist watchlist. Despite failing to plead any such claims in his complaint, he nonetheless seeks, among other relief, "a declaratory judgment that Defendants placed Mr. Nur on the watchlist illegally and unlawfully imposed consequences tied to that status." Compl. ¶ 140.

This is a puzzling juxtaposition. Because alleged TSDS status is at the core of Plaintiff's complaints about the border inspections he has experienced and expects to experience in the future, it would stand to reason that Plaintiff would base his claims on the TSDS determination, either directly or indirectly. But Plaintiff has failed to bring a direct count challenging the basis for his alleged inspection encounters, and his stand-alone, unadorned request for TSDS relief is untethered from his claims. For these reasons, dismissal is warranted.[13]

CONCLUSION

For the foregoing reasons, pursuant to Rule 12(b)(6), Plaintiff's Fourth Amendment, Fifth Amendment, and APA claims should be dismissed for failure to state a claim.

[13] Should the Court construe the Complaint as challenging Plaintiff's alleged TSDS status (or should Plaintiff re-plead), Defendants would likely seek dismissal of such an as-yet-un-pleaded claim. If the Court did not dismiss such a claim, that may warrant judicial review of a record supporting any TSDS status, if it exists, not any discovery. *See Trinity Am. Corp. v. E.P.A.*, 150 F.3d 389, 401 n. 4 (4th Cir. 1998) ("Review of agency action is limited to the administrative record before the agency when it makes its decision."). Moreover, as is common in cases implicating sensitive national security information, such review may involve submission of materials for the Court's review *ex parte* and *in camera*. *See, e.g.*, *Jifry v. FAA*, 370 F.3d 1174, 1181-82 (D.C. Cir. 2004); *Scherfen v. U.S. Dep't of Homeland Sec.*, No. 3:08-cv-1554, 2010 WL 456784, at *4, 7-8 (M.D. Pa. Feb. 2, 2010); *see also, e.g., Bassiouni v. FBI*, 436 F.3d 712, 722 n.7 (7th Cir. 2006).

Dated: July 11, 2022

Respectfully submitted,

JESSICA D. ABER
United States Attorney

BRIAN M. BOYNTON
Principal Deputy Assistant Attorney General
Civil Division

ANTHONY J. COPPOLINO
Deputy Director, Federal Programs Branch

BRIGHAM J. BOWEN
Assistant Director, Federal Programs Branch

MADELINE MCMAHON
ALEXANDER N. ELY
Trial Attorneys
United States Department of Justice
Civil Division, Federal Programs Branch
1100 L St NW
Washington, DC 20530
Tel: (202) 514-2395

/s/ *Lauren A. Wetzler*
LAUREN A. WETZLER
Chief, Civil Division
Assistant United States Attorney
Office of the United States Attorney
2100 Jamieson Ave.
Alexandria, VA. 22314
Tel: (703) 299-3752
Fax: (703) 299-3983
Lauren.Wetzler@usdoj.gov

Counsel for Official Capacity Defendants